



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------|-------------|----------------------|---------------------|------------------|
|-----------------|-------------|----------------------|---------------------|------------------|

10/596,887

06/28/2006

Satoshi Kitani

112857-914

1891

29175 7590
K&L Gates LLP
P. O. BOX 1135
CHICAGO, IL 60690

06/16/2009

EXAMINER

SQUIRES, BRETT S

ART UNIT

PAPER NUMBER

2431

MAIL DATE

DELIVERY MODE

06/16/2009

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

| | | | |
|------------------------------|--------------------------------------|--|--|
| Office Action Summary | Application No. 10/596,887 | Applicant(s) KITANI, SATOSHI | |
| | Examiner BRETT SQUIRES | Art Unit 2431 | |

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 25 February 2009.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1 and 3-5 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1 and 3-5 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

Art Unit: 2431

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

2. Claims 1 and 3-5 are rejected under 35 U.S.C. 103(a) as being obvious over Ochi et al. (WO 2003/038571 A1) in view of Lynn et al. (US 5,345,508). The examiner respectfully points out that for the purposes of the present Office action US 7,275,161 is taken to be the English language equivalent of WO 2003/038571 A1.

Regarding Claim 1:

Ochi discloses a data processing system having transfer controlling means for controlling transfer of data ("Recording Medium Authentication Data Transmission Unit" and "Authentication Unit" See fig. 1 ref. nos. 12 and 14), counting means ("Authentication Unit" See fig. 1 ref. no. 14) for counting the number of time the transfer controlling means has controlled the transfer of the data ("The authentication unit also updates mutual authentication processing data stored in the data storage unit such as the mutual authentication processing count." See col. 14 lines 25-28), first determining means ("Recording Medium Authentication Data Transmission Unit" See fig. 1 ref. no. 12) for determining whether the number of time counted by the counting means is at least equal to a maximum count ("The recording medium authentication data transmission unit judges whether the number of times mutual authentication processing has been executed has reached a predetermined number." See col. 12 lines 36-51),

Art Unit: 2431

first instructing means ("Recording Medium Authentication Data Transmission Unit" See fig. 1 ref. no. 12) which if the number of times is found at least equal to the maximum count by the first determining means then gives the transfer controlling means an instruction to stop the transfer of the data ("If the predetermined number has been reached the recording medium authentication data transmission unit notifies the user to this effect and ends the processing." See col. 12 lines 36-51), second determining means ("Recording Medium Authentication Data Reception Unit" See fig. 1 ref. no. 31) for determining whether an instruction to have the initializing vector supplied is given by an external apparatus ("Data processing device" See figs. 1 and 3 ref. no. 10 and "The data processing device is, for example, a general purpose computer such as a personal computer," See col. 12 lines 4-11) to and from which is sent and received the data of which the transfer is controlled by the transfer controlling means ("According to the stated structure continuous data transfer is not permitted unless the recording medium receives predetermined data." See col. 4 lines 51-60), second instructing means ("Encrypted Data Transmission Unit" See fig. 1 ref. no. 33) which if the instruction to have the initializing vector supplied is found given by the second determining means then giving the counting means an instruction to reset the number of times having been counted ("The counting unit may reset the number each time predetermined data is received from the data processing device. See col. 4 lines 48-50), and outputting means ("Recording Medium Authentication Data Transmission Unit" See fig. 1 ref. no. 12) which if the instruction is given by the first instructing means then outputs to the external apparatus a message saying that the transfer of the data is stopped ("If the

Art Unit: 2431

predetermined number has been reached, the medium authentication data transmission unit notifies the user to this effect and ends processing ." See col. 13 lines 36-51).

Ochi does not disclose generating means for generating an initializing vector for use in either encrypting or decrypting the data of which the transfer is controlled by the transfer controlling means and second instructing means which if the instruction to have the initializing vector supplied is found given by the second determining means then gives the generating means an instruction to generate the initializing vector.

Lynn discloses an apparatus for variable overhead cached encryption having a generating means ("Initialization Vector Generator" See fig. 2 ref. no. 29) for generating an initializing vector for use in encryption and decrypting the which data the transfer is controlled ("The initialization vector is combined with a key using an XOR gate to produce a temporal key for which acts as a seed for a Pseudorandom number generator. The Pseudorandom number is then combined with Plain text data using an XOR gate." See col. 5 lines 1-49) and second instructing means ("Counter" See fig. 2 ref. no. 21) which if the instruction to have the initializing vector supplied is found given by the second determining means then gives the generating means an instruction to generate the initializing vector ("The counter controls the generation of new initialization vectors." See col. 5 lines 40-68 and col. 6 lines 1-23).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the data processing system disclosed by Ochi to use variable overhead cached encryption for encrypting the authentication data transmitted between the data processing device and the information recording medium such as that taught

Art Unit: 2431

by Lynn in order to perform high speed encryption of the transmitted data (See Lynn col. 2 lines 47-51).

Regarding Claims 3-5:

Ochi discloses a data processing system for controlling transfer of data ("Data Processing Device," "Connection Device," and "Information Recording Medium" See fig. 1 ref. nos. 10, 20, and 30), counting the number of times the transfer controlling step has controlled the transfer of the data ("The authentication unit also updates mutual authentication processing data stored in the data storage unit such as the mutual authentication processing count." See col. 14 lines 25-28), firstly determining whether the number of times counted in the counting step is at least equal to a maximum count ("The recording medium authentication data transmission unit judges whether the number of times mutual authentication processing has been executed has reached a predetermined number." See col. 12 lines 36-51), if the number of times is found at least equal to the maximum count in the first determining step then firstly giving in the transfer controlling step an instruction to stop the transfer of the data ("If the predetermined number has been reached the recording medium authentication data transmission unit notifies the user to this effect and ends the processing." See col. 12 lines 36-51), secondly determining whether an instruction to have the initializing vector supplied is given by an external apparatus ("Data processing device" See figs. 1 and 3 ref. no. 10 and "The data processing device is, for example, a general purpose computer such as a personal computer," See col. 12 lines 4-11) to and from which is sent and received the data of which the transfer is controlled in the transfer controlling step ("According to the

Art Unit: 2431

stated structure continuous data transfer is not permitted unless the recording medium receives predetermined data.” See col. 4 lines 51-60), if the instruction to have the initializing vector supplied is found given in the second determining step then secondly giving in said counting step an instruction to reset the number of times having been counted (“The counting unit may reset the number each time predetermined data is received from the data processing device. See col. 4 lines 48-50), and if the instruction to stop the transfer of the data is given in the transfer controlling step, then outputting to the external apparatus a message saying that the transfer of the data is stopped (“If the predetermined number has been reached, the medium authentication data transmission unit notifies the user to this effect and ends processing .” See col. 13 lines 36-51).

Ochi does not disclose generating an initializing vector for use in either encrypting or decrypting the data of which the transfer is controlled in the transfer controlling step and if the instruction to have the initializing vector supplied is found given in the second determining step then secondly giving in the generating step an instruction to generate the initializing vector.

Lynn discloses a method for variable overhead cached encryption for generating an initializing vector for use in encrypting and decrypting the data of which the transfer is controlled in the transfer controlling step (“The initialization vector is combined with a key using an XOR gate to produce a temporal key for which acts as a seed for a Pseudorandom number generator. The Pseudorandom number is then combined with Plain text data using an XOR gate.” See col. 5 lines 1-49) and if the instruction to have the initializing vector supplied is found given in the second determining step then

Art Unit: 2431

secondly giving in the generating step an instruction to generate the initializing vector ("The counter controls the generation of new initialization vectors." See col. 5 lines 40-68 and col. 6 lines 1-23).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the data processing system disclosed by Ochi to use variable overhead cached encryption for encrypting the authentication data transmitted between the data processing device and the information recording medium such as that taught by Lynn in order to perform high speed encryption of the transmitted data (See Lynn col. 2 lines 47-51).

Response to Arguments

3. Applicant's arguments filed February 25, 2009 have been fully considered but they are not persuasive.

In response to applicant's argument that Ochi does not teach outputting to the external apparatus a message saying that the transfer of data is stopped, the examiner respectfully points out that the use of the data stored on a memory card is permitted only when the personal computer and the memory card authenticate each other as being legitimate (See col. 11 lines 50-65). Therefore, a mutual authentication processing failed signal indicates that the transfer of data between memory card and the personal computer has stopped. The mutual authentication failed signal is generated by the recording medium authentication data transmission unit (See col. 13 lines 35-51) and output to the components of the personal computer that perform read

Art Unit: 2431

processing and write processing ("Card Slot" See fig. 1 ref. no. 20 and "Data transmission performed according to software such as firmware incorporated into integrated circuits." col. 12 lines 20-27) in addition to the components of the personal computer that generate a screen display alerting the user that mutual authentication processing failed (See fig. 3).

In response to applicant's argument that Ochi does not teach notifying a user that the transfer of data has stopped, the examiner respectfully disagrees with the applicant's argument. The examiner points out that Ochi teaches notifying a user when mutual authentication processing fails (See figure 3 and col. 13 lines 36-51) and in response to mutual authentication processing failing the data processing device stops read processing and write processing with the information recording medium (See col. 13 lines 52-67). The examiner further points out that use of data stored on the information recording medium is permitted only when the personal computer and the memory card authenticate each other as being legitimate (See col. 11 lines 50-64). Therefore, a message stating that mutual authentication processing failed tells the user that no read or write processing can occur with the mutual authentication failure being the reason why.

In response to applicant's argument that one of ordinary skill in the art would not combine Ochi's data processing device and information recording medium into a single information processing apparatus as claimed, the examiner respectfully points out that applicant's argument is not supported by the claim language. The examiner respectfully points out that the claim language "An information processing apparatus" does not limit

Art Unit: 2431

the scope of the claim to a disc drive unit (See Applicant's specification fig. 10 ref. no. 301), but instead limits the scope of the claim any structure that performs information processing.

Conclusion

4. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRETT SQUIRES whose telephone number is (571) 272-8021. The examiner can normally be reached on 9:30am - 6:00pm Monday - Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on (571) 272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2431

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/BS/

/William R. Korzuch/
Supervisory Patent Examiner, Art Unit 2431